(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 984 404 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
08.03.2000 Bulletin 2000/10

(51) Int. Cl.[7]: **G07F 7/10**, G06K 19/073

(21) Application number: **99113202.8**

(22) Date of filing: **08.07.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **02.09.1998 DE 19839847**

(71) Applicant:
International Business Machines Corporation
Armonk, NY 10504 (US)

(72) Inventors:
- **Hamann, Ernst-Michael, Dipl.-Ing.**
  71034 Böblingen (DE)
- **Kaisser, Michael, Dipl.-Ing.**
  71088 Holzgerlingen (DE)

(74) Representative:
Teufel, Fritz, Dipl.-Phys.
IBM Deutschland Informationssysteme GmbH,
Patentwesen und Urheberrecht
70548 Stuttgart (DE)

(54) Storing data objects in a smart card memory

(57) The invention refers to a method for storing data objects 210, 220, 230, 240 in the memory 200 of a smart card 100. To do this, general and application-specific data objects are defined using freely selectable security characteristics and access rights, which are filed in the memory of a smart card which is divided into several application-specific memory areas 110, 120 so that data objects with identical access conditions are located in one and the same memory area, irrespective of the application program 310, 320, 330 or smart card user 400 to which these data objects are allocated. All application programs and the smart card user can access the data objects irrespective of the corresponding access conditions. In this way, the re-issuing of smart cards in the case of later expansion of the file structure of the smart card for an application or the addition of extra applications is not necessary. The smart card user can allow any applications to store data on his smart card.

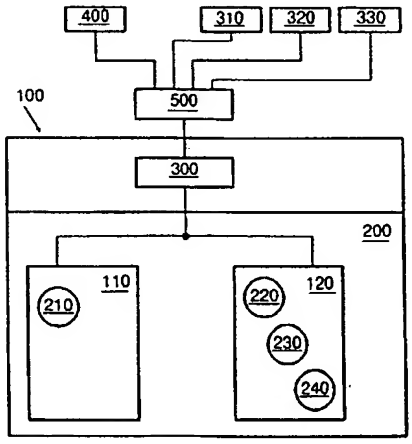

FIG. 2

EP 0 984 404 A2

Description

[0001] The invention refers to a method for storing data objects in a smart card memory.

[0002] Intelligent data carriers consisting of a microprocessor (chip) and memory units are already known. They are used, for example, as application-specific smart cards (bank cards, ID cards, etc.). File structures in accordance with the application programs are defined in the manufacture of the smart cards. It is therefore difficult to carry out additional applications and file structures at a later date. The smart card user can solely use the smart card for the applications stated on the issuing of the card. The later expansion of file structures for an application or the addition of later applications often means that a smart card has to be reissued.

[0003] Application programs for these smart cards must be aware of the smart card to be used as well as the file structures on them in order to be able to use them. In addition, the applications must control the specific interfaces for the smart card readers and smart cards in order to be able to access the file structures of the smart card. An additional disadvantage can be found in each application having a prescribed place for storing data objects available to it which cannot be altered in size. This issuing of static memory limits the extent of data to be stored in an application and greatly restricts the flexibility of each application. In addition, up until now two separate interfaces have had to be implemented for the use of simple data access, and for cryptographic methods.

[0004] The cryptographic token interface standard (PKCS#11) of RSA Data Security Inc. sets out a general application interface standard for cryptographic units. This standard can also be applied to smart card readers and smart cards in order to address cryptographic characteristics of these components. In this, the management and use of objects such as symmetrical and asymmetrical codes and certificates for these codes are possible. The code objects can then be used for cryptographic methods such as the marking, coding and decoding of data.

[0005] It is the task of the present invention to make available a method which removes the disadvantages of the current state of technology. In particular, one task of the invention is to make available a method which allows application programs and smart card users to create, manage and use data objects on a smart card independent of the smart card operating system and the smart card readers used. An additional task of the invention is to allow the smart card user to check the data structure of the smart card and to allow several applications to store data objects on its smart card. In addition, one task of the present invention is to allow the smart card user to equip data objects with any security characteristics and access conditions.

[0006] In accordance with the invention, this task is solved by the characteristics of the independent claims. Additional preferred embodiments of the present invention are described in the subclaims.

[0007] In accordance with the present invention, general and application-specific data objects are defined using freely selectable security characteristics and access conditions which are filed in the smart card memory, which is divided into several application-independent memory areas, so that data objects with identical access conditions are located in one and the same memory areas, irrespective of the application program or smart card user to which the data objects are allocated. All applications and the smart card user can access the data objects irrespective of the corresponding access conditions.

[0008] The present invention allows application interfaces to the application programs and the smart card user to be made available for the creation, management and use of data objects on the smart card, irrespective of the smart card operating system and the smart card reader used.

[0009] These generic smart cards can be used for all applications selected by the smart card user. The user is also able to allow several applications to store data objects on his smart card. The issuing of a new smart card is not necessary in the case of an additional application being selected. The use of new applications is limited solely by the size of the memory available for data objects on the smart card. The memory available for a certain application is no longer set to a maximum size from the start. It is simply limited by the size of the overall memory of the smart card. The application operators are saved the costs of issuing application-specific smart cards. The costs for setting up smart card-specific reading devices and application interfaces only occur once for all applications. An additional important advantage is that the data structure of the smart card can be controlled by the smart card user. In addition, data objects can be protected from improper use in whole or in part by passwords or cryptographic methods. The security characteristics and access conditions of a data object can be set as required in the data object system both during the initialisation of the smart card as well as by an application or by the smart card user. With the introduction of public coding methods, such a smart card can also be used for identifying the smart card user for applications in public networks such as the Internet. The data objects can be filed in secure smart card data memories in mobile operation, for example in a network. This allows the smart card user to make mobile use of the data objects using with his identity established cryptographically using public codes and certification. In addition, only one common application interface is required for data access and for cryptographic methods.

[0010] The invention is described in the following using preferred embodiments. The figures show the following:

Fig. 1 a simplified schematic view of the smart card

including the application environment according to the current state of technology;

Fig. 2 a simplified schematic view of the smart card including the application environment in accordance with the present invention.

[0011] As shown in Fig. 1, the manufacturer of the smart card has, according to the state of current technology, already established areas 11, 12, 13 within the smart card memory during the definition and manufacture of the smart card, to which certain applications 31, 32, 33 are allocated. In these application-specific memory areas 11, 12, 13, application-specific data objects 21, 22, 23 are filed and protected in a respective application. In this, communication takes place through application interfaces 5. The methods necessary for creating the file structures and the type and method of use of the file structures by the operating system 3 and the application programs 31, 32, 33 and thus the later use of the smart card by the smart card user 4 are already ascertained on issuing the smart card.

[0012] As shown in Fig. 2, the invention is designed to define any general and application-specific data objects 210, 220, 230, 240 of different types using freely selectable security characteristics and access conditions. These data objects 210, 220, 230, 240 of different types can be defined in any way either in creating the smart card 100 or afterwards by the smart card user 400 or by application programs 310, 320, 330 through an application interface 500 and securely filed and modified in generally available memory areas 110, 120 on the smart card 100 without requiring an application-specific file structure on the smart card.

[0013] In defining the data object during or after the manufacture of the smart card, any data objects can be created, for example general or application-specific. In this, data objects can be standardised and equipped with data contents even during the manufacture of the smart card. In defining the data objects by the smart card user 400 after the manufacture of the smart card, freely selectable data objects can be created according to the requirements of the smart card user. Alternatively, the smart card user 400 can select defined data objects in the creation of the smart card and add data to them. In addition, after the smart card manufacture, individual applications 310, 320, 330 can create data objects or add data to data objects already created. These data objects can be accessed by the different applications or the smart card user through an application interface 500 according to the access conditions assigned to it. In this way it is irrelevant which sort of data objects are being dealt with. For example, they can be data objects of the accessing application, another application or general, i.e. non-application-specific data objects. If the data objects are those with certain access conditions such as private data objects of the smart card user, then access under the control of the smart card user is carried out using a password. Also, data objects can be defined which are equally available to several applications and the smart card user.

[0014] This concept results in an application-independent intelligent smart card with open file structures which can, however, be controlled by the smart card user. Examples of data objects on the present invention are data objects of the following types:

Visitor cards (V-CARD) 210, lists of addresses in the Internet (BOOKMARK) 220, log-on dates of an application (LOGIN) 230, smart card user notes (NOTE) 240.

[0015] Preferably, an application interface 500 is adapted to the smart card 100 using the PKCS#11 standard for cryptographic units. It is advantageous that this standard also knows objects in the "data" class in addition to objects in the "code" and "certification" classes, whose structures are generally determined by cryptographic standards.

[0016] The PKCS#11 standard is thus expanded so that in addition to the use of cryptographic methods it also allows the checking of general and application-specific data objects 210, 220, 230, 240 with freely selectable security characteristics and access rights for application programs 310, 320, 330.

[0017] The data to be stored in the data objects and additional details such as the data type, security characteristics and access rights, are established by the application program or by the smart card user and transmitted to the application interface. From the data received by the application interface, data objects can be defined, for example, using the command "create_object" of the PKCS#11 standard. In this, the attributes "APPLICATION", "PRIVATE" and "VALUE" used in the PKCS#11 standard can be used. In the "APPLICATION" attribute, for example the type of the data object and security characteristics which describe the type of data file in the "VALUE" attribute, can be established as encoded or marked. In the "PRIVATE" attributes, one or more access conditions such as password interrogation can be established. In this way, for example, it can be established whether it is a private, a public or a data object with another access condition. In the "VALUE" attribute, the data of the data object can be established. The file structure on the smart card is simplified by all data objects with identical access conditions being filed in one and the same memory area which is identified by this access condition. This occurs independently of the application, or by which smart card user the respective data object was created. An allocation of the smart card memory 200 to certain applications 310, 320, 330 is not carried out. The memory areas 110, 120 replace the memory areas previously required in which data objects of a certain application were combined.

[0018] Reading, writing, modification, sorting and deleting of data objects 210, 220, 230, 240 in the mem-

ory areas 110, 120 and additional use of data objects can be carried out using methods known to the skilled person. If the data of a data object is structured in an established way, for example, according to a general usual standard which can be the case with the V-CARD data object, then these can be stored in a "Tag length value" structure. Variable lengths in data objects are thus facilitated in this way and the smart card memory 200 can be better used to capacity.

[0019] There is at least one, and preferably several of these memory areas 110, 120 whose number and size can be ascertained on initiating the smart card. In this, the memory areas have a preferred size of at least 1000 bytes, or more preferably 2000 bytes. In a particularly preferred embodiment, the size of the memory areas are at least 4000 bytes respectively.

[0020] During manufacture of the smart card, an access condition or a combination of different access conditions is allocated to each of these application-independent memory areas 110, 120. This can be, for example, a log-in procedure with password interrogation. If the memory areas are those which can be accessed without any conditions, then the access condition can also be "no condition". In a preferred embodiment, one of the application-independent memory areas 110 has the attribute "public" and another memory area 120 the attribute "private". In this way, all data objects filed in the pubic memory area 110, i.e. public data objects 210, can be accessed on logging on without the smart card user 400 being identified. During this time, all data objects which are filed in the private memory area 120, i.e. private data objects 220, 230, 240 cannot be accessed until a log-in procedure with a valid password has been carried out by the smart card user 400. As all data objects in a memory area are based on the same access conditions, the private memory area 120 and all the data objects 220, 230, 240 located in it are therefore protected in this case by a password. It would also be possible, for example, to have a memory area which can be written not by the smart card user but only by a security representative such as the smart card manufacturer.

[0021] The access conditions of the memory areas can be filed in separate areas of the smart card memory. They are checked and monitored by the smart card operating system and by the application interface. The individual applications have no influence here on the access conditions of individual memory areas. It would be possible for critical applications to file data objects in an additional application-independent memory area which has additional or other access conditions. Alternatively in this case, it would be possible to have, in addition to the application-independent memory areas 110, 120, the use of a normal memory area with regard to the application, in which exclusively all data objects of the critical application are combined.

[0022] In addition to the application-independent memory areas 110, 120 there are additional memory areas in which the serial number of the smart card, the codes and passwords are filed.

[0023] The present invention permits the use of a number of checks, some of which can be combined with one another. For example, data objects of a certain type can only be filed on the creation of the smart card, i.e. only filed when the smart card is personalized. One example is a verification code which can be used for checking the validity of the smart card in which a test question is marked by this code.

[0024] Additional data objects of a certain type may only be filed, amended or read after authentication in user-mode, i.e. after a log-in procedure with a valid user password. This applies particularly to the data objects of a private memory area.

[0025] Again, additional data objects of a certain type may only be filed, amended or read after authentication in a security representative mode, i.e. after a log-in procedure with a valid security representative password. An example is a "licence to call up an application" type.

[0026] Other data objects of a certain type may only be filed in a private data area. One example is the LOGIN type.

[0027] Again, other data objects of a certain type can only be changed by applications with knowledge of a special access code. For other applications, these data objects can only be accessed in read mode. Data objects can be marked by the creator of the data object using a private code including the serial number of the smart card. The application which later uses the data object can then check using the public code of the creator and the serial number of the smart card to see whether the data object has the correct origin, has not been changed and also has not been copied by another smart card. This allows the storing of a unique "ticket", e.g. an entry card or a medication prescription, on the smart card.

[0028] In addition, it is possible to encode the whole data object or only particularly confidential parts of the data object during creation. In this way, the confidentiality of the data object in transmission to and from the smart card by the application is ensured. One example is the LOGIN type in which the user password can be filed in encrypted form.

[0029] In a preferred embodiment of the present invention, certain data objects 210, 220, 230, 240 can trigger direct actions by means of suitable application programs 310, 320, 330 when selected using a graphic user interface, such as the starting of an application by the LOGIN type, starting an Internet browser using the BOOKMARK type or opening the address-book function using the V-CARD type.

[0030] In an additional preferred embodiment, instead of the data objects, program objects such as Java Applets can be stored on the smart card. The present invention can be applied not only to smart cards but also to any intelligent data carrier.

[0031] Cryptographic co-processors with their own

memory management (crypto-adapters), such as are found on a computer disk, can be used for example, instead of a smart card. Alternatively, crypto-adapters can also be used in a program form.

Claims

1. Method for storing data objects in the memory of a smart card, characterised by the following steps:

   a) defining at least one data memory area (110, 120) in the memory (200) of the smart card (100), where at least one access condition is allocated to each data memory area (110, 120)

   b) receiving data to be stored, which is provided with certain access conditions,

   c) defining data objects (210, 220, 230, 240) from the data to be stored,

   d) storing the data objects in one of the data memory areas (110, 120) so that all data objects with identical access conditions are stored in one and the same data memory area to which the corresponding access condition is allocated, irrespective of the application program (310, 320, 330) or smart card user (400) to which the data object is allocated.

2. Method according to claim 1, characterised in that the steps a) to d) are carried out during the manufacture of the smart card.

3. Method according to claim 1, characterised in that the steps b) to d) are carried out by the smart card user (400) through an application interface (500).

4. Method according to claim 1, characterised in that the steps b) to d) are carried out by an application program (310, 320, 330) through an application interface (500).

5. Method according to claim 1, characterised in that during the definition of data objects any general and application-specific data objects can be defined.

6. Method according to claim 1, characterised in that the data to be stored is provided with security characteristics.

7. Method according to claim 6, characterised in that the data objects are protected in whole or in part by cryptographic methods according to the security characteristics of the data to be stored.

8. Method according to claim 6, characterised in that the access conditions and security characteristics of the data to be stored are established in a freely selectable way.

9. Method according to claim 8, characterised in that the access condition is the confirmation of a password.

10. Application interface (500) for use of cryptographic methods during communication between a smart card (100) and an application program (310, 320, 330) or smart card user (400), characterised in that it comprises additional data object structures such that general and application-specific data objects (210, 220, 230, 240) with freely selectable security characteristics and access conditions can be used.

11. Smart card (100) with data memory areas (110, 120) characterised in that at least one access condition is allocated to each data memory area (110, 120).

12. Smart card according to claim 11, characterised in that data objects (210, 220, 230, 240) are stored in said data memory areas (110, 120) independent of the application program (310, 320, 330) or smart card user (400) allocated to it.

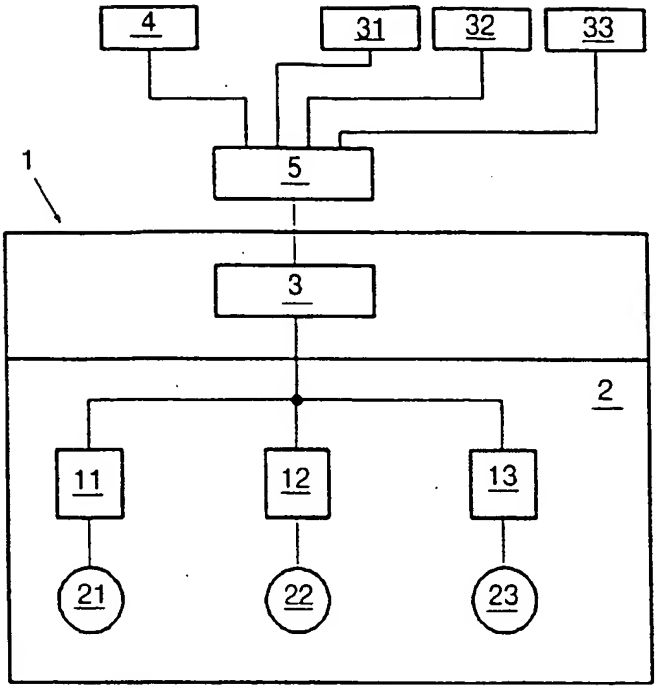
4
31
32
33
1
5
3
2
11
12
13
21
22
23

FIG. 1

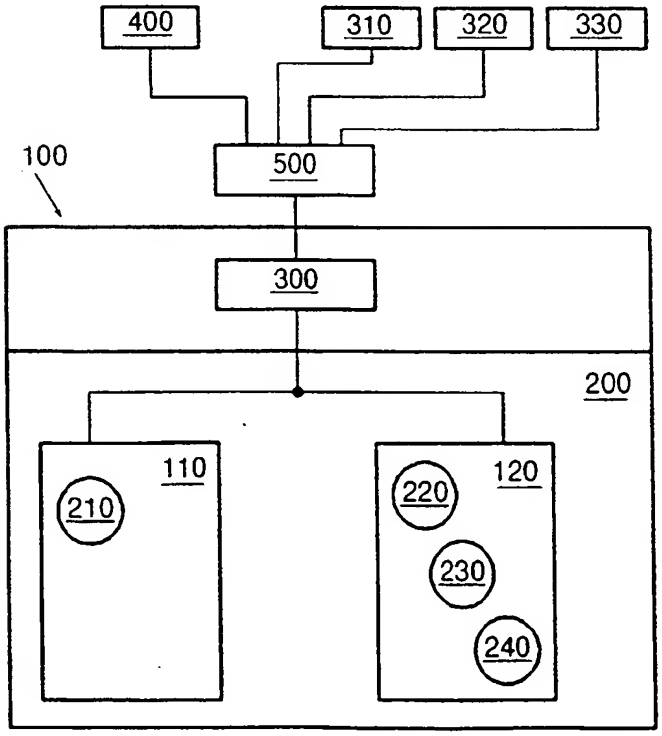
400
310
320
330
100
500
300
200
110
210
120
220
230
240

FIG. 2